

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002164899 A**

(43) Date of publication of application: **07.06.02**

(51) Int. Cl.  
**H04L 12/28**  
**H04L 12/24**  
**H04L 12/26**  
**H04L 29/14**

(21) Application number: **2000358073**  
(22) Date of filing: **24.11.00**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**  
(72) Inventor: **SASAKI TAKETO**  
**SHINOHARA TOSHIAKI**

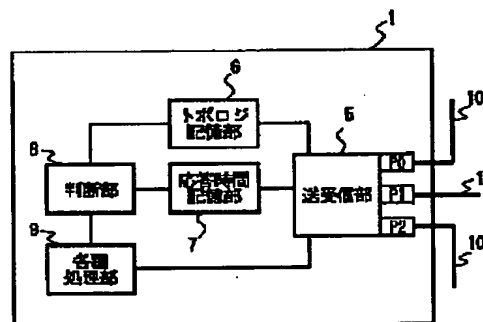
**(54) NETWORK MONITORING METHOD AND ITS EQUIPMENT**

**(57) Abstract:**

**PROBLEM TO BE SOLVED:** To provide a network monitoring method and its equipment for finding and taking countermeasure against disguise of a device.

**SOLUTION:** The network monitoring equipment of the invention is provided with a topology memory part 6 which stores topological information of the network, a response time memory part 7 which stores obtained response time after execution of a response inspection command, and a decision part 8 which decides the consistency between the topological information stored in the topology memory part 6 and the response time stored in the response time memory part 7, and it finds and takes a countermeasure against disguise of a device in a network like IEEE1394 by which such topology can be obtained.

COPYRIGHT: (C)2002,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-164899  
(P2002-164899A)

(43) 公開日 平成14年6月7日 (2002.6.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコ-ト*(参考)
H 0 4 L	12/28	H 0 4 L 11/00	3 1 0 A 5 K 0 3 0
	12/24	11/08	5 K 0 3 3
	12/26	13/00	3 1 3 5 K 0 3 5
	29/14		

審査請求 未請求 請求項の数55 O L (全 28 頁)

(21) 出願番号 特願2000-358073 (P2000-358073)

(22) 出願日 平成12年11月24日 (2000. 11. 24)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 佐々木 雄飛

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(72) 発明者 篠原 利章

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(74) 代理人 100072604

弁理士 有我 軍一郎

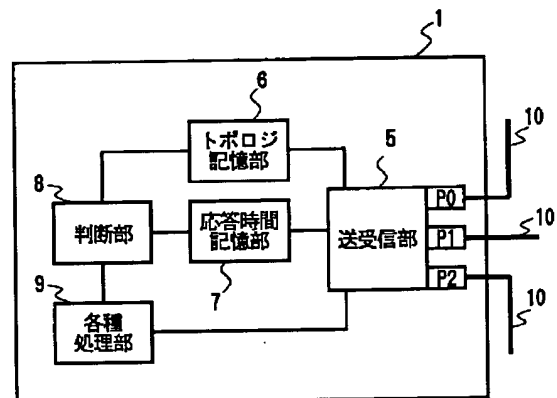
最終頁に続く

(54) 【発明の名称】 ネットワーク監視方法および装置

(57) 【要約】

【課題】 機器のなりすましを発見並びに対策するネットワーク監視方法および装置を提供すること。

【解決手段】 本発明のネットワーク監視装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部6と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部7と、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶された応答時間との整合性を判断する判断部8とを備え、I E E 1 3 9 4 のようなトポロジが得られるネットワークにおいて機器のなりすましを発見し対策を行う。



【特許請求の範囲】

【請求項1】 ネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することを特徴とするネットワーク監視方法。

【請求項2】 ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記記憶されたトポロジ情報と、前記記憶された応答時間との整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項3】 ネットワークのトポロジ情報を記憶し、パケットを受信したポートを識別し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記識別されたポートと前記識別されたソースIDの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項4】 ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記ネットワークのバスの状態が、grant状態からdata prefix状態に変化するまでの時間を測定し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記記憶された応答時間と、前記測定された時間と前記識別されたソースIDの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項5】 ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記ネットワークのバスの状態が、data end状態からrequest状態に変化するまでの時間を測定し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースIDとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項6】 ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースIDとの組み合わせとの整合性を判

断することで、がネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項7】 ネットワークのトポロジ情報を記憶し、連続してパケットを受信した場合に、この受信した各パケットのソースIDとその受信順番を識別し、前記記憶されたトポロジ情報と、前記受信したパケットのソースIDと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項8】 ネットワークのトポロジ情報を記憶し、ACKとデータパケットを連続して受信した場合に、この受信した各パケットのソースIDとその受信順番を識別し、前記記憶されたトポロジ情報と、前記受信したパケットのソースIDと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項9】 ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定し、受信ACKパケットのソースノードを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたACKパケットのソースノードとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視方法。

【請求項10】 前記識別されたソースIDがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、前記ソースIDと前記ルーティングテーブルとが矛盾する場合を発見することを特徴とする請求項3乃至請求項8の何れかに記載のネットワーク監視方法。

【請求項11】 受信パケットのソースIDを識別し、この識別されたソースIDがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、前記ソースIDと前記ルーティングテーブルとが矛盾する場合を発見することを特徴とする請求項9に記載のネットワーク監視方法。

【請求項12】 バスリセットをトリガとして、判断に使用する情報の収集を開始することを特徴とする請求項2乃至請求項11の何れかに記載のネットワーク監視方法。

【請求項13】 矛盾を発見した場合に、前記パケットを破棄することを特徴とする請求項2乃至請求項12の何れかに記載のネットワーク監視方法。

【請求項14】 矛盾を発見した場合に、前記パケット

を破壊することを特徴とする請求項2乃至請求項12の何れかに記載のネットワーク監視方法。

【請求項15】 矛盾を発見した場合に、バスリセットを発生させることを特徴とする請求項2乃至請求項12の何れかに記載のネットワーク監視方法。

【請求項16】 矛盾を発見した場合に、警告を発生することを特徴とする請求項2乃至請求項12の何れかに記載のネットワーク監視方法。

【請求項17】 矛盾を発見した場合に、ポートを切り離すことを特徴とする請求項2乃至請求項12の何れかに記載のネットワーク監視方法。

【請求項18】 ネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することを特徴とするネットワーク監視装置。

【請求項19】 ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項20】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットを受信したポートを識別するポート識別部と、前記受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ポート識別部に識別されたポートと前記ソース識別部に識別されたソースIDの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項21】 複数のポータルを持つブリッジを含むネットワーク監視装置において、前記ブリッジが、ルーティング情報を記憶するルーティング記憶部と、パケットを受信したポータルを識別するポータル識別部と、前記受信パケットのソースIDを識別するソース識別部と、前記ルーティング記憶部に記憶されたルーティング情報と、前記ポータル識別部で識別されたポータルと前記ソース識別部で識別されたソースIDの組み合わせとの整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項22】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、

バスの状態がgrant状態からdata prefix状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別された前記ソースIDの組み合わせとの整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項23】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、

バスの状態がdata end状態からrequest状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソースIDとの組み合わせの情報の整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項24】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、

ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、

バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソ-

スIDの組み合わせとの整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項25】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、

ネットワークのトポロジ情報を記憶するトポロジ記憶部と、

パケットの連続を受信した場合に、それぞれのパケットのソースIDとその受信順番を識別するソース順番識別部と、

前記トポロジ記憶部に記憶されたトポロジ情報と、前記ソース順番識別部で識別されたソースIDとその受信順番との整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項26】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、

ネットワークのトポロジ情報を記憶するトポロジ記憶部と、

ACKとデータパケットの連続を受信した場合に、それぞれのパケットのソースIDとその受信順番を識別するACKソース順番識別部と、

前記トポロジ記憶部に記憶されたトポロジ情報と、前記ACKソース識別部で識別されたソースIDとその受信順番との整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項27】 少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、

ネットワークのトポロジ情報を記憶するトポロジ記憶部と、

応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、

バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定する時間測定部と、

受信ACKパケットのソースノードを識別するソース識別部と、

前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたACKパケットの前記ソースノードの組み合わせとの整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とするネットワーク監視装置。

【請求項28】 ブリッジのルーティングテーブルを確

認するルーティングテーブル確認部と、

前記ソース識別部で識別されたソースIDと、前記ルーティングテーブル確認部で確認されたブリッジの前記ルーティングテーブルとの整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とする請求項20乃至請求項26の何れかに記載のネットワーク監視装置。

【請求項29】 パケットのソースIDを識別するソース識別部と、

ブリッジのルーティングテーブルを確認するルーティングテーブル確認部と、

前記ソース識別部で識別されたソースIDと、前記ルーティングテーブル確認部で確認されたブリッジの前記ルーティングテーブルとの整合性を判断する判断部とを具備し、

ネットワークトポロジ上矛盾する場合を発見することを特徴とする請求項27に記載のネットワーク監視装置。

【請求項30】 バスリセットをトリガとして、前記判断部で使用する情報の収集を開始することを特徴とする請求項19乃至請求項29の何れかに記載のネットワーク監視装置。

【請求項31】 矛盾を発見した場合に、前記パケットを破棄するパケット破棄処理部を具備することを特徴とする請求項19乃至請求項30の何れかに記載のネットワーク監視装置。

【請求項32】 矛盾を発見した場合に、前記パケットを破壊するパケット破壊処理部を具備することを特徴とする請求項19乃至請求項30の何れかに記載のネットワーク監視装置。

【請求項33】 矛盾を発見した場合に、バスリセットを発生させるバスリセット発生処理部を具備することを特徴とする請求項19乃至請求項30の何れかに記載のネットワーク監視装置。

【請求項34】 矛盾を発見した場合に、警告を発生する警告発生処理部を具備することを特徴とする請求項19乃至請求項30の何れかに記載のネットワーク監視装置。

【請求項35】 矛盾を発見した場合に、ポートを切り離すポート接続制御処理部を具備することを特徴とする請求項19乃至請求項30の何れかに記載のネットワーク監視装置。

【請求項36】 ネットワークのトポロジ情報を記憶し、  
パケットのデスティネーションIDを識別し、  
前記トポロジ情報と前記デスティネーションIDの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピータするポートと、ダミー情報をリピータするポートとを決定することを特徴とするリピータ方法。

【請求項37】 バスリセットをトリガとして、前記情報の収集を開始することを特徴とする請求項36に記載のリピート方法。

【請求項38】 ネットワークのトポロジ情報を記憶するトポロジ記憶部と、  
パケットのデスティネーションIDを識別するデスティネーション識別部と、  
前記トポロジ記憶部に記憶されたトポロジ情報と前記デスティネーション識別部で識別されたデスティネーションIDの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピートするポートと、ダミー情報をリピートするポートとを決定するポート制御部とを具備することを特徴とするリピータ装置。

【請求項39】 バスリセットをトリガとして、前記情報の収集を開始することを特徴とする請求項38に記載のリピータ装置。

【請求項40】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態をユーザに通知することを特徴とするネットワーク保護方法。

【請求項41】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴とするネットワーク保護方法。

【請求項42】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を記録することを特徴とするネットワーク保護方法。

【請求項43】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴とするネットワーク保護方法。

【請求項44】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴とするネットワーク保護方法。

【請求項45】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのパケットのルーティングを、設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴とするネットワーク保護方法。

【請求項46】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、関連する機器に対し機器認証を行う、またはやり直すことを特徴とするネットワーク保護方法。

【請求項47】 請求項16に記載のネットワーク監視方法からの警告の発生を受けて、データの暗号化を行

う、または暗号化キーを再作成することを特徴とするネットワーク保護方法。

【請求項48】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、  
警告発生時の状態を収集する情報収集部と、  
この収集された情報をユーザに通知する表示部とを具備し、  
警告時に警告の内容と前記警告発生時の状態をユーザに通知することを特徴とするネットワーク装置。

【請求項49】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、  
警告発生時の状態を収集する情報収集部と、  
公衆回線に接続された公衆回線通信部とを具備し、  
警告時に警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴とするネットワーク装置。

【請求項50】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、  
警告発生時の状態を収集する情報収集部と、  
情報を記録する記憶部とを具備し、  
警告時に警告の内容と警告発生時の状態を記録することを特徴とするネットワーク装置。

【請求項51】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、  
警告に関連する機器の挙動または状態を収集する情報収集部と、  
情報を記録する記憶部とを具備し、  
警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴とするネットワーク装置。

【請求項52】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、  
他機器にサービスを提供するサービス処理部と、  
条件によりサービスの提供の許可を行うサービス制御部とを具備し、  
警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴とするネットワーク装置。

【請求項53】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、  
パケットのルーティングを行うルーティング部と、  
ルーティングの設定を行うルーティング制御部とを具備し、  
警告に関連した機器の何れかまたは全てからのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴とするネットワーク装置。

【請求項54】 請求項34に記載のネットワーク監視装置からの警告を受ける警告受信部と、

機器の認証機能を備えた機器認証部とを具備し、関連する機器に対し機器認証を行う、またはやり直すことを特徴とするネットワーク装置。

【請求項５】 請求項３４に記載のネットワーク監視装置からの警告を受ける警告受信部と、データの暗号化を行う暗号部とを具備し、データの暗号化を行う、または暗号化キーを再作成することを特徴とするネットワーク装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークのセキュリティを強化するネットワーク監視方法および装置に関し、特に、IEEE 1394に代表されるバス型ネットワークにおけるセキュリティを強化するネットワーク監視方法および装置に関する。

【０００２】

【従来の技術】IEEE 1394はシンプルな構成と高いパフォーマンスにより、家庭内LANなど今後の様々な機器間接続手段として期待されている。100Mbps以上の転送速度、Isochronousと呼ばれるマルチメディアデータ転送に適した転送方式、機器の接続を自動的に認識することで、ネットワークの移動中に機器を追加、削除が可能な活線接続機能を備え、ツリー型のネットワークを構成し広い用途に活用することが可能である。

【０００３】用途のひとつにカメラを用いた監視システムを構成することが考えられる。これは、高速な転送速度のために多量の映像等のデータを伝送することが可能になるためである。

【０００４】従来の監視システムの場合、監視に必要な数のアナログ出力カメラと、それと同数のビデオキャプチャボード等のA/D変換機構とを必要とし、また、カメラとビデオキャプチャボードとの接続に一本のケーブルを必要とし、カメラ台数と同じ本数のケーブルを引き回す必要があった。

【０００５】一方、IEEE 1394を利用した監視システムの場合、監視に必要な数のIEEE 1394対応デジタル出力カメラに対し、監視装置として受信、記録のためのパソコンを最低ひとつ接続するだけで済み、またツリー型のネットワークを構成することにより、少ないケーブル本数で監視システムを構成することが可能となった。

【０００６】

【発明が解決しようとする課題】しかし、このような従来のIEEE 1394は、バス型ネットワークであり、送出されたパケットは基本的にバス上の全てのノードに届く。これにより、本来パケットを受信する必要の無い機器にパケットを盗聴される可能性があるという問題があった。

【０００７】また、バス上の全てのノードにパケットが

届くことが前記とされているため、パケット上のソースIDの記述を確認する以外にパケットを送出したノードを特定する機構が無く、パケット上のソースIDの記述を偽られるという問題があった。

【０００８】IEEE 1394を用いて監視システムを構築する場合、制御コマンドや秘匿性の高い情報など重要なパケットについて、その送出ノードおよび受信ノードが信用できる機器であることが保障されていることが望ましい。

【０００９】しかし上記問題はパケットの送受信に関わる機器の特定を妨げ、機器のなりすましを可能にするため、監視システムのセキュリティレベルを下げることになる。

【００１０】本発明はこのような問題を解決するためになされたもので、機器のなりすましを発見並びに対策する方法および装置を提供するものである。

【００１１】

【課題を解決するための手段】本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１２】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記記憶されたトポロジ情報と、前記記憶された応答時間との整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１３】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、パケットを受信したポートを識別し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記識別されたポートと前記識別されたソースIDの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【００１４】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記ネットワークのバスの状態が、grant状態からdata prefix状態に変化するまでの時間を測定し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記記憶された応答時間と前記測定された時間と前記識別されたソースIDの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見

することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0015】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、前記ネットワークのバスの状態が、data end状態からrequest状態に変化するまでの時間を測定し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースIDとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0016】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定し、受信パケットのソースIDを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたソースIDとの組み合わせとの整合性を判断することで、がネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0017】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、連続してパケットを受信した場合に、この受信した各パケットのソースIDとその受信順番を識別し、前記記憶されたトポロジ情報と、前記受信したパケットのソースIDと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0018】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ACKとデータパケットを連続して受信した場合に、この受信した各パケットのソースIDとその受信順番を識別し、前記記憶されたトポロジ情報と、前記受信したパケットのソースIDと前記受信順番の整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0019】また、本発明のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、応答検査コマンドを実行して、得られた応答時間を記憶し、バスの状態

がdata end状態からdata prefix状態に変化するまでの時間を測定し、受信ACKパケットのソースノードを識別し、前記記憶されたトポロジ情報と、前記測定した時間と前記識別されたACKパケットのソースノードとの組み合わせとの整合性を判断し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0020】また、上記ネットワーク監視方法は、受信パケットのソースIDを識別し、この識別されたソースIDがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、前記ソースIDと前記ルーティングテーブルとが矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0021】また、上記ネットワーク監視方法は、バスリセットをトリガとして、判断に使用する情報の収集を開始することを特徴としている。これにより、なりすまされている機器となりすましを行っている機器の候補が、少ない情報収集回数で判別できることとなる。

【0022】また、上記ネットワーク監視方法において、矛盾を発見した場合に、前記パケットを破棄しても良い。また、矛盾を発見した場合に、前記パケットを破壊しても良い。あるいは、矛盾を発見した場合に、バスリセットを発生させても良い。これにより、なりすましが行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【0023】また、上記ネットワーク監視方法において、矛盾を発見した場合に、警告を発生しても良い。これにより、なりすましが行なわれている可能性を上位レイヤや他の機器に知らせることができ、他機器あるいはユーザに注意を促すことができることとなる。

【0024】さらに、上記ネットワーク監視方法は、矛盾を発見した場合に、ポートを切り離しても良い。これにより、なりすましを行っている機器の候補をバスから強制的に排除することができることとなる。

【0025】さらに、本発明のネットワーク監視装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することを特徴としている。この構成により、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0026】また、本発明のネットワーク監視装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、前記トポロジ記憶部に記憶



されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。この構成により、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0027】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットを受信したポートを識別するポート識別部と、前記受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ポート識別部に識別されたポートと前記ソース識別部に識別されたソースIDの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0028】また、本発明のネットワーク監視装置は、複数のポータルを持つブリッジを含むネットワーク監視装置において、前記ブリッジが、ルーティング情報を記憶するルーティング記憶部と、パケットを受信したポータルを識別するポータル識別部と、前記受信パケットのソースIDを識別するソース識別部と、前記ルーティング記憶部に記憶されたルーティング情報と、前記ポータル識別部で識別されたポータルと前記ソース識別部で識別されたソースIDの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0029】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がgrant状態からdata prefix状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別された前記ソースIDの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できる

こととなる。

【0030】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がdata end状態からrequest状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソースIDとの組み合わせの情報の整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0031】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定する時間測定部と、受信パケットのソースIDを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたソースIDの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0032】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットの連続を受信した場合に、それぞれのパケットのソースIDとその受信順番を識別するソース順番識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ソース順番識別部で識別されたソースIDとその受信順番との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0033】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワ

ーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、ACKとデータパケットの連続を受信した場合に、それぞれのパケットのソースIDとその受信順番を識別するACKソース順番識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記ACKソース識別部で識別されたソースIDとその受信順番との整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0034】また、本発明のネットワーク監視装置は、少なくとも一つのポートを持つリピータを含むネットワーク監視装置において、前記リピータが、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、応答検査コマンドを実行して、得られた応答時間を記憶する応答時間記憶部と、バスの状態がdata end状態からdata prefix状態に変化するまでの時間を測定する時間測定部と、受信ACKパケットのソースノードを識別するソース識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と、前記応答時間記憶部に記憶された応答時間と、前記時間測定部で測定した時間と前記ソース識別部で識別されたACKパケットの前記ソースノードの組み合わせとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0035】上記のネットワーク監視装置は、パケットのソースIDを識別するソース識別部と、ブリッジのルーティングテーブルを確認するルーティングテーブル確認部と、前記ソース識別部で識別されたソースIDと、前記ルーティングテーブル確認部で確認されたブリッジの前記ルーティングテーブルとの整合性を判断する判断部とを具備し、ネットワークトポロジ上矛盾する場合を発見することを特徴としている。これにより、バス上に存在する機器のうち、なりすまされている機器となりすましを行っている機器の候補が判別できることとなる。

【0036】上記のネットワーク監視装置は、バスリセットをトリガとして、前記判断部で使用する情報の収集を開始することを特徴としている。これにより、なりすまされている機器となりすましを行っている機器の候補が少ない情報収集回数で判別できることとなる。

【0037】上記のネットワーク監視装置において、矛盾を発見した場合に、前記パケットを破棄するパケット破棄処理部を具備しても良い。また、矛盾を発見した場合に、前記パケットを破壊するパケット破壊処理部を具備しても良い。あるいは、矛盾を発見した場合に、バスリセットを発生させるバスリセット発生処理部を具備しても良い。これにより、なりすましが行なわれていた場

合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【0038】上記のネットワーク監視装置において、矛盾を発見した場合に、警告を発生する警告発生処理部を具備しても良い。これにより、なりすましが行なわれている可能性を上位レイヤや他の機器に知らせることができ、他機器あるいはユーザに注意を促すことができることになる。

【0039】上記のネットワーク監視装置において、矛盾を発見した場合に、ポートを切り離すポート接続制御処理部を具備しても良い。これにより、なりすましを行っている機器の候補をバスから強制的に排除することができることとなる。

【0040】さらに、本発明のリピータ方法は、ネットワークのトポロジ情報を記憶し、パケットのデスティネーションIDを識別し、前記トポロジ情報と前記デスティネーションIDの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピータするポートと、ダミー情報をリピータするポートとを決定することを特徴としている。これにより、なりすましや盗聴が行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【0041】また、上記のリピータ方法において、バスリセットをトリガとして、前記情報の収集を開始しても良い。これにより、なりすましや盗聴が行なわれていた場合に少ない情報収集回数で、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【0042】また、本発明のリピータ装置は、ネットワークのトポロジ情報を記憶するトポロジ記憶部と、パケットのデスティネーションIDを識別するデスティネーション識別部と、前記トポロジ記憶部に記憶されたトポロジ情報と前記デスティネーション識別部で識別されたデスティネーションIDの組み合わせ情報に基づいて、ポートの状態を判断し、前記パケットをリピータするポートと、ダミー情報をリピータするポートとを決定するポート制御部とを具備することを特徴としている。これにより、なりすましや盗聴が行なわれていた場合に、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【0043】また、上記リピータ装置において、バスリセットをトリガとして、前記情報の収集を開始することを特徴としている。これにより、なりすましや盗聴が行なわれていた場合に少ない情報収集回数で、そのトランザクションの完成を妨げる可能性を高めることができることとなる。

【0044】本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態をユーザに通知することの特徴としている。これにより、ユーザに速やかに、なりすましが行なわれている可能性を示すことができることとな

る。

【0045】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴としている。これにより、遠隔地のユーザに速やかに、なりすましが行なわれている可能性を示すことができることとなる。

【0046】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告の内容と警告発生時の状態を記録することを特徴としている。これにより、なりすましの証拠とその時の状況を保存することができることとなる。

【0047】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴としている。これにより、不正な機器について継続的に監視を行うことができることとなる。

【0048】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴としている。これにより、不正な機器に提供するサービスを、通常と異なるものにすることができることとなる。

【0049】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、警告に関連した機器の何れかまたは全てからのパケットのルーティングを、設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴としている。これにより、不正な機器の通信の扱いを、通常と異なるものにすることができることとなる。

【0050】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、関連する機器に対し機器認証を行う、またはやり直すことを特徴としている。これにより、不正の疑いのある機器が発見された場合に、不正な機器と正常な機器との確認ができることとなる。

【0051】また、本発明のネットワーク保護方法は、上記ネットワーク監視方法からの警告の発生を受けて、データの暗号化を行う、または暗号化キーを再作成することを特徴としている。これにより、不正の疑いのある機器が発見された場合に、セキュリティを厳しくすることができることとなる。

【0052】本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告発生時の状態を収集する情報収集部と、この収集された情報をユーザに通知する表示部とを具備し、警告時に警告の内容と前記警告発生時の状態をユーザに通知することを特徴としている。これにより、ユーザに速やかに、

なりすましが行なわれている可能性を示すことができることになる。

【0053】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告発生時の状態を収集する情報収集部と、公衆回線に接続された公衆回線通信部とを具備し、警告時に警告の内容と警告発生時の状態を公衆回線を経由してユーザに通知することを特徴としている。これにより、遠隔地のユーザに速やかに、なりすましが行なわれている可能性を示すことができることとなる。

【0054】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告発生時の状態を収集する情報収集部と、情報を記録する記憶部とを具備し、警告時に警告の内容と警告発生時の状態を記録することを特徴としている。これにより、なりすましの証拠とその時の状況を保存することができることとなる。

【0055】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、警告に関連する機器の挙動または状態を収集する情報収集部と、情報を記録する記憶部とを具備し、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録することを特徴としている。これにより、不正な機器について継続的に監視を行うことができることとなる。

【0056】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、他機器にサービスを提供するサービス処理部と、条件によりサービスの提供の許可を行うサービス制御部とを具備し、警告に関連した機器の何れかまたは全てからのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することを特徴としている。これにより、不正な機器に提供するサービスを、通常と異なるものにすることができることとなる。

【0057】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、パケットのルーティングを行うルーティング部と、ルーティングの設定を行うルーティング制御部とを具備し、警告に関連した機器の何れかまたは全てからのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更することを特徴としている。これにより、不正な機器の通信の扱いを、通常と異なるものにすることができることとなる。

【0058】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、機器の認証機能を備えた機器認証部とを具備し、関連する機器に対し機器認証を行う、またはやり直すことを特徴としている。これにより、不正の疑いのある機器が発見された場合に、不正な機器と正常な機器との確認

ができることとなる。

【0059】また、本発明のネットワーク装置は、上記ネットワーク監視装置からの警告を受ける警告受信部と、データの暗号化を行う暗号部とを具備し、データの暗号化を行う、または暗号化キーを再作成することの特徴としている。これにより、不正の疑いのある機器が発見された場合に、セキュリティを厳しくすることができることとなる。

【0060】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。尚、全ての図面において、同様な構成要素は同じ参照記号および符号を用いて示してある。

(第1の実施の形態)

【0061】図1に示すように、本発明の第1の実施の形態のネットワーク監視装置1は、送受信部5と、トポロジ記憶部6と、応答時間記憶部7と、判断部8と、各種処理部9とを備えている。本実施の形態において、送受信部5はポートP0、ポートP1、ポートP2の三ポートを有するものとするが、これに限定されるものではない。ポートP0～P2はそれぞれバス10に接続されている。

【0062】トポロジ記憶部6は、送受信部5を介してネットワークのトポロジ情報を収集し、記憶するものである。応答時間記憶部7は、送受信部5を介してネットワーク上のノードに応答検査コマンドであるpingを実行し、ネットワーク監視装置1とその他のノードとの間のpingに対する応答時間（以下、「ping時間」と呼ぶ）を記憶するものである。pingを行う順番は、どのようなものでも構わない。判断部8は、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報とを比較し、矛盾が存在するかどうかを判断するものである。各種処理部9は、判断部8で、矛盾が存在すると判断された場合、後述する各種処理を行うものである。

【0063】上記のトポロジ情報の収集およびpingの実施は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0064】このように構成されたネットワーク監視装置1の動作を以下に説明する。

【0065】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、応答時間記憶部7により、送受信部5を介してネットワーク上のノードにpingが実行され、ネットワーク監視装置1とその他のノードとの間のping時間が記憶される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記

憶されたping時間情報とが比較され、矛盾が存在するかどうか判断される。矛盾が存在すると判断された場合、各種処理部9により各種処理が行なわれる。

【0066】図2に示すネットワークを例にして、本実施の形態のネットワーク監視装置1の判断部8による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置1からなる。ID=0のノード201のping時間はID=2のノード203のping時間よりも長いはずであり、その差は（PHY遅延+ケーブル遅延）に等しいはずである。この条件を満たしていない場合、判断部8は、トポロジ情報記憶部6に記憶されているトポロジ情報と、ping時間情報との間に矛盾が存在すると判断する。すなわち、ID=0のノード201またはID=2のノード203は、「他のノードに、なりすまされている」と考えられる。これをネットワーク全体に行うことにより、ネットワーク上のノードを正常なノードと不正なノードに判別することが可能である。以後、「不正なノード」とは、「なりすましを行っているノード」、「なりすましが行なわれているノード」のうちの何れかまたは全てを示す。

【0067】また、例えばID=2のノード203のping時間とID=5のノード205のping時間とが等しかった場合、ID=5のノード205がID=2のノード203になりすましを行っている可能性があることが解る。

【0068】以上のように、本発明の第1の実施の形態のネットワーク監視装置1は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、pingを実行して、得られたping時間を記憶する応答時間記憶部7と、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報とを比較し、矛盾が存在するかどうかを判断する判断部8と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補を発見することができる。

【0069】各種処理部9が行う処理としては、以下のものが考えられる。

【0070】各種処理部9は、判断部8で矛盾が発見された場合にパケットを破棄するパケット破棄処理部（図示無し）を有しても良い。各種処理部9のパケット破棄処理部は、不正なノードから送出されたパケットを破棄するように送受信部5を制御する。パケットを破棄するとは、受信したパケットを上位層に渡さないことと、受信したパケットをそのままリピーターせずにダミーや一部を書き換え無害にしたパケットをリピーターの代わりに送出することを示す。

【0071】また、各種処理部9のパケット破棄処理部は、不正なノードに対し、送出されたパケットを全て破

棄させるようにしても良い。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。さらに、ネットワーク監視装置1よりも下流に存在するノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【0072】あるいは、各種処理部9は、判断部8で矛盾が発見された場合にパケットを破壊するパケット破壊処理部（図示無し）を有しても良い。各種処理部9のパケット破壊処理部は、不正なノードから送出されたパケットを破壊するように、送受信部5を制御する。パケットを破壊するとは、受信したパケットを上位層に渡さないことと、パケットがバス上に存在する場合でも関係なくバスをドライブすることを示す。ここで、ドライブする状態としては、パケットデータ状態と衝突する状態であり、例えば、IDOL、TX\_DATA\_END、TX\_DATA\_PREFIX、TX\_REQUEST、およびBUS\_RESET等がある。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。さらに、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【0073】あるいは、各種処理部9は、判断部8で矛盾が発見された場合にバスリセットを発生させるバスリセット発生処理部（図示無し）を有しても良い。各種処理部9のバスリセット発生処理部は、バスリセットを発生させるように送受信部5を制御する。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することもできる。

【0074】あるいは、各種処理部9は、判断部8で矛盾が発見された場合に警告を発生する警告発生処理部（図示無し）を有しても良い。各種処理部9の警告発生処理部が発生する警告はネットワーク監視装置1の上位層に対して出されても良いし、送受信部5を介してネットワーク上の他のノードに出されても良い。なりすまされていることを報告するという点からなりすまされているノードに警告しても良い。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードが存在することを知ることができる。また、ネットワーク上のノードが、不正の疑いのあるノードが存在することを知ることができる。さらに、ネットワーク上のノードが、なりすましをされているということを知ることができる。

【0075】あるいは、各種処理部9は、判断部8で矛盾が発見された場合にポートを切り離すポート接続制御処理部（図示無し）を有しても良い。各種処理部9のポート接続制御処理部は、ポートを使用しないように送受

信部5を制御する。この時使用を停止するポートは不正なノードに繋がっているポートである。

【0076】図2の例で言うと、なりすましを行っているのがID=5のノード205であった場合、ポートP1の機能を停止させることで、ID=5のノード205をバスに参加させないことが可能である。これにより不正の疑いのあるノードをバスから排除することができる。

【0077】このように、各種処理部9は、矛盾を発見した場合に、なりすまして送出されたパケット等を破壊、破壊等を行うことで、なりすましによるトランザクションの完了を防ぎ、さらに、なりすましの可能性を警告することで、他の機器あるいはユーザに注意を促すことが可能である。また、各種処理部9は、矛盾を発見した場合に、なりすまし機器を切り離し、バスに参加させないことで、なりすましを防止することができる。

（第2の実施の形態）

【0078】図3は、本発明の第2の実施の形態のネットワーク監視方法を示すフローチャートを示す。同図に示すように、ステップS101において、ネットワークのトポロジ情報を獲得する。ステップS102において、ネットワーク上のノードについてpingを実行し、ping時間を獲得する。ステップS103において、ステップS101で獲得したトポロジ情報とステップS102で獲得したping時間を比較し、矛盾が存在するかどうかを判断する。矛盾が存在しなかった場合、ステップS104へ進み、バスリセットの発生を待機する。矛盾が存在した場合、ステップS105に進み、後述する各種処理を行う。ステップS105の各種処理が終了した後は、ステップS104へ進む。ステップS104において、バスリセットが検出された場合、ステップS101へ戻る。

【0079】図2に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップS103における判断の方法を説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置1からなる。ID=0のノード201のping時間はID=2のノード203のping時間よりも長いはずであり、その差は（PHY遅延+ケーブル遅延）に等しいはずである。この条件を満たしていない場合、ステップS103で、ステップS101で獲得したトポロジ情報と、ステップS102で獲得したping時間情報との間に矛盾が存在すると判断する。すなわち、ID=0のノード201またはID=2のノード203は、「他のノードに、なりすまされている」と考えられる。これをネットワーク全体に行うことにより、ネットワーク上のノードを、正常なノードと不正なノードに判別することが可能である。

【0080】また、例えばID=2のノード203のping時間と、ID=5のノード205のping時間

とが等しかった場合、ID=5のノード205がID=2のノード203になりすましを行っている可能性があることが解る。

【0081】以上のように、本発明の第2実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、pingを実行して、得られたping時間を記憶し、記憶されたトポロジ情報と、記憶されたping時間との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

【0082】ステップS105で行なわれる各種処理としては、以下のものが考えられる。

【0083】ステップS103で矛盾が発見された場合に、ステップS105において、不正なノードから送出されたパケットを破棄しても良い。パケットを破棄するとは、受信したパケットを上位層に渡さないことと、受信したパケットをそのままリピーターせずにグミヤ一部を書き換え無害にしたパケットをリピーターの替わりに送出することを示す。

【0084】また、ステップS105において、不正なノードに対し、送出されたパケットを全て破棄させるようにしても良い。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク監視装置1よりも下流に存在するノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【0085】あるいは、ステップS103で矛盾が発見された場合に、ステップS105において、不正なノードから送出されたパケットを破壊しても良い。パケットを破壊するとは、受信したパケットを上位層に渡さないことと、パケットがバス上に存在する場合でも関係なくバスをドライブすることを示す。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【0086】あるいは、ステップS103で矛盾が発見された場合に、ステップS105において、バスリセットを発生させても良い。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードからのパケットを受信することを防止することができる。また、ネットワーク上のノードが、不正の疑いのあるノードからのパケットを受信することを防止することができる。

【0087】あるいは、ステップS103で矛盾が発見された場合に、ステップS105において、警告を発生しても良い。警告は上位層に対して出されても良いし、ネットワーク上の他のノードに出されても良い。なりす

まされていることを報告するという点から、なりすまされているノードに警告しても良い。これによりネットワーク監視装置1の上位層が、不正の疑いのあるノードが存在することを知ることができる。また、ネットワーク上のノードが、不正の疑いのあるノードが存在することを知ることができる。また、ネットワーク上のノードが、なりすましをされているということを知ることができる。

【0088】あるいは、ステップS103で矛盾が発見された場合に、ステップS105において、ポートを切り離し、ポートの使用を停止しても良い。この時使用を停止するポートは不正なノードに繋がっているポートである。

【0089】図2の例で言うと、なりすましを行っているのがID=5のノード205であった場合、ポートP1の機能を停止させることで、ID=5のノード205をバスに参加させないことが可能である。これにより不正の疑いのあるノードをバスから排除することができる。

【0090】このように、ステップS103で矛盾を発見した場合に、ステップS105における各種処理において、なりすまして送出されたパケット等を破棄、破壊等を行うことで、なりすましによるトランザクションの完了を防ぎ、さらに、なりすましの可能性を警告することで、他の機器あるいはユーザに注意を促すことが可能である。また、各種処理部9は、矛盾を発見した場合に、なりすまし機器を切り離し、バスに参加させないことで、なりすましを防止することができる。

(第3の実施の形態)

【0091】図4は、本発明の第3の実施の形態のネットワーク監視装置21の概略ブロック図を示す。これは上記第1の実施の形態とは、応答時間記憶部7の替わりに、ソース識別部11を設けた点が相違している。第1の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0092】ソース識別部11は、送受信部5を介してパケットを受信した際に、そのパケットのソースIDとパケットを受信したポートを識別するものである。

【0093】以下に、本実施の形態のネットワーク監視装置21の動作を説明する。

【0094】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、ソース識別部11により、パケットが受信され、パケットのソースIDとパケットを受信したポートが識別される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、ソース識別部11が識別したパケットのソースIDとパケットを受信したポートとが比較され、矛盾が存在するかどうか判断される。矛盾が存在すると判断された場合、各種処理部9により、上記第1の実施の形態と同様な各種処理が行われる。こ

れにより、本実施の形態においても第1の実施の形態と同様な効果が得られる。

【0095】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0096】図2に示すネットワークを例にして、本実施の形態のネットワーク監視装置21の判断部8による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置21からなる。ソースIDがID=0のノード201から送出されたパケットは、ネットワークトポロジ上、必ずポートP0を介して受信されるはずである。これがポートP0以外のポートを介して受信された場合、ID=0のノード201は他のノードになりすまされていると考えられる。

【0097】以上のように、本発明の第2の実施の形態のネットワーク監視装置21は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、送受信部5を介してパケットを受信した際に、そのパケットのソースIDとパケットを受信したポートを識別するソース識別部11と、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報とを比較し、矛盾が存在するかどうかを判断する判断部8と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードが接続されているポートを発見することができる。

(第4の実施の形態)

【0098】図5は、本発明の第4の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第2の実施の形態とは、ステップS102およびS103の替わりに、ステップS111乃至ステップS113を設けた点が主に相違している。

【0099】同図に示すように、ステップS101において、ネットワークのトポロジ情報を獲得する。次いでステップS104において、バスリセットの発生を待機する。ステップS104において、バスリセットが検出された場合、ステップS101へ戻り、検出されない場合はステップS111へ進む。ステップS111において、パケットの受信を待機する。ステップS111において、パケットが受信されない場合は、ステップS104へ戻り、パケットが受信された場合、ステップS112へ進む。

【0100】ステップS112において、パケットを受信したポートとパケットのソースIDを識別する。次いでステップS113において、ステップS101で獲得

したトポロジ情報とステップS112で識別したパケットのソースIDとパケットを受信したポートとを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップS105に進み、各種処理を行う。ステップS105における各種処理は、図3に示された上記第2の実施の形態におけるステップS105の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第2の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップS104へ戻る。ステップS105の各種処理が終了した後も、ステップS104へ戻る。

【0101】図2に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップS113における判断の方法を説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置21からなる。ソースIDがID=0のノード201から送出されたパケットは、ネットワークトポロジ上、必ずポートP0を介して受信されるはずである。これがポートP0以外のポートを介して受信された場合、ID=0のノード201は他のノードになりすまされていると考えられる。

【0102】以上のように、本発明の第4の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、パケットを受信したポートを識別し、受信したパケットのソースIDを識別し、記憶されたトポロジ情報と、識別された記憶されたポートとソースIDの組み合わせとの整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードが接続されているポートとを発見することができる。

(第5の実施の形態)

【0103】図6は、本発明の第5の実施の形態のネットワーク監視装置31の概略ブロック図を示す。これは上記第1の実施の形態とは、さらにソース識別部11と時間測定部12を設けた点が相違している。上記の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0104】時間測定部12は、送受信部5を介してバス上の状態が変化した時間を測定するものである。測定される時間については後述する。

【0105】以下に、本実施の形態のネットワーク監視装置31の動作を説明する。

【0106】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、応答時間記憶部7により、送受信部5を介してネットワーク上のノードにpingが実行され、ネットワーク監視装置31とその他のノードとの間のping時間が記憶される。ここで、pingを行う順番はどのようなものでも構わない。

【0107】次に、ソース識別部11により、パケット

が受信され、パケットのソースIDとパケットを受信したポートが識別される。さらに、時間測定部12により、送受信部5を介してバス上の状態が変化した時間が測定される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報と、ソース識別部11に識別されたソースID情報と、時間測定部12が測定したバス状態時間測定情報とが比較され、矛盾が存在するかどうか判断される。矛盾が存在すると判断された場合、各種処理部9により、上記第1の実施の形態と同様な各種処理が行なわれる。これにより、本実施の形態においても第1の実施の形態と同様な効果が得られる。

【0108】上記のトポロジ情報の収集およびpingの実施は、設定された時間毎に行なわれても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行なわれても良い。バスリセット発生毎に行なわれるのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0109】図2に示すネットワークを例にして、本実

$$\text{PHY遅延} \times 4 + \text{ケーブル遅延} \times 4 + \text{ping時間} \quad \dots \text{式(1)}$$

【0112】ソースID=0のパケットを受信した時に、その直前のgrant-dataprefix間時間が上記の式(1)の値と異なる場合、そのパケットはID=0のノード201が送出したものではないと考えられる。

【0113】また、その際のgrant-data p

$$\text{PHY遅延} \times 2 + \text{ケーブル遅延} \times 2 + \text{ping時間} \quad \dots \text{式(2)}$$

時間測定部12が測定する時間は、grant-dataprefix間時間以外にも、data end-request間時間、data end-dataprefix間時間あるいは、data end-ACKのdataprefix間時間が考えられる。

【0115】また、これらはルートノードが正常であることを前提とした場合であり、ルートノードが不正なノードである可能性を考慮すると、request-grant間時間や、request-dataprefix間時間も判断の材料となる。従って、時間測定部12は、request-grant間時間または、request-dataprefix間時間を測定しても良く、これにより、ルートノードが不正なノードである場合も同様な効果が得られることとなる。

【0116】以上のように、本発明の第5の実施の形態のネットワーク監視装置31は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、pingを実行して、得られたping時間を記憶する応答時間記憶部7と、送受信部5を介してパケットを受信した際に、そのパケットのソースIDとパケットを受信したポートを識別するソース識別部11と、送受信部5を介してバス上の状態が変化した時間を測定する時間測定部12と、ト

施の形態のネットワーク監視装置31の判断部8による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置31からなる。

【0110】ID=0のノード201がパケットを送出する場合には、以下の手順を行う。最初に、パケットを送出するためにバスの利用権を得たい旨を、上流のバス状態をrequest状態にドライブすることにより知らせる。次に、ルートノード(この場合はID=10のノード210)がID=0のノード201への経路のバス状態をgrant状態にドライブする。grant状態を検知したID=0のノード201は、バスをdataprefix状態にドライブし、パケットの送出を開始する。この時、ネットワーク監視装置31から見た場合、バス状態がgrant状態に変化してからdataprefix状態に変化するまでに、おおよそ下記の式(1)の時間が経過するはずである。

【0111】

refix間時間が、下記の式(2)であった場合、この値はID=2のノード203がパケット送出する場合の値と一致するため、ID=2のノード203がID=0のノード201になりすましていると考えられる。

【0114】

ポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報と、ソース識別部11で識別されたソースIDと、時間測定部12で測定された時間とを比較し、矛盾が存在するかどうかを判断する判断部8と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補を発見することができる。

(第6の実施の形態)

【0117】図7は、本発明の第6の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第2の実施の形態とは、ステップS103の替わりに、ステップS121乃至ステップS123を設けた点が主に相違している。

【0118】同図に示すように、ステップS101において、ネットワークのトポロジ情報を獲得する。次いでステップS102において、ネットワーク上のノードについてpingを実行し、ping時間を獲得する。次いで、ステップS104において、バスリセットの発生を待機する。ステップS104において、バスリセットが検出されなかった場合、ステップS101へ戻り、検出された場合は、ステップS121へ進む。

【0119】ステップS121において、バス状態の変



化時間を測定する。ここで測定される時間については後述する。次いでステップS122において、パケットを受信したポートとパケットのソースIDを識別する。次いでステップS123において、ステップS101で獲得したトポロジ情報と、ステップS102で獲得した応答時間と、ステップS121で測定したバス状態の変化時間情報と、ステップS122で識別したパケットのソースID情報とが比較され、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップS105で各種処理を行う。ステップS105における各種処理は、図3に示された上記第2の実施の形態におけるステップS105の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第2の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップS104へ戻る。ステップS105の各種処理が終了した後も、ステップS104へ戻る。

【0120】図2に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップS123に

$$\text{PHY遅延} \times 4 + \text{ケーブル遅延} \times 4 + \text{ping時間} \quad \cdots \text{式(3)}$$

【0123】ソースID=0のパケットを受信した時に、その直前のgrant-dataprefix間時間が上記の式(3)の値と異なる場合、そのパケットはID=0のノード201が送出したものではないと考えられる。

【0124】また、その際のgrant-data p

$$\text{PHY遅延} \times 2 + \text{ケーブル遅延} \times 2 + \text{ping時間} \quad \cdots \text{式(4)}$$

【0126】ステップS121で測定する時間は、grant-data prefix間時以外にも、data end-request間時間、data end-data prefix間時間あるいは、data end-ACKのdataprefix間時間が考えられる。

【0127】また、これらはルートノードが正常であることを前提とした場合であり、ルートノードが不正なノードである可能性を考慮すると、request-grant間時間や、request-data prefix間時間も判断の材料となる。従って、ステップS121では、request-grant間時間または、request-data prefix間時間を測定しても良く、これにより、ルートノードが不正なノードである場合も同様な効果が得られることとなる。

【0128】以上のように、本発明の第6の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、pingを実行して、得られたping時間を記憶し、パケットを受信したポートを識別し、受信したパケットのソースIDを識別し、バス上の状態が変化した時間を測定し、記憶されたトポロジ情報と、記憶されたping時間と、識別された記憶されたソースIDと、測定された時間との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノ

おける判断の方法を説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置31からなる。

【0121】ID=0のノード201がパケットを送出する場合には、以下の手順を行う。最初にパケットを送出するためにバスの利用権を得たい旨を、上流のバス状態をrequest状態にドライブすることで知らせる。次に、ルートノード(この場合はID=10のノード210)がID=0のノード201への経路のバス状態をgrant状態にドライブする。grant状態を検知したID=0のノード201は、バスをdataprefix状態にドライブし、パケットの送出を開始する。この時、ネットワーク監視装置31から見た場合、バス状態がgrant状態に変化してからdataprefix状態に変化するまでに、おおよそ下記の式(3)の時間が経過するはずである。

【0122】

refix間時間が下記の式(4)であった場合、この値はID=2のノード203がパケット送出する場合の値と一致するため、ID=2のノード203がID=0のノード201になりすましていると考えられる。

【0125】

ドと、なりすましを行っているノードの候補とを発見することができる。

(第7の実施の形態)

【0129】図8は、本発明の第7の実施の形態のネットワーク監視装置41の概略ブロック図を示す。これは上記第1の実施の形態とは、応答時間記憶部7の替わりに、ソース順番識別部13を設けた点が相違している。第1の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0130】ソース順番識別部13は、連続したパケットを受信した際に、受信したパケットのソースIDとその受信順番を識別するものである。

【0131】以下に、本実施の形態のネットワーク監視装置41の動作を説明する。

【0132】始めに、ネットワークのトポロジ情報が受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、ソース順番識別部13により、連続したパケットが受信された場合に、その連続したパケットのソースIDとその受信順番が識別される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、ソース順番識別部13識別されたパケットのソースIDとその受信順番とが比較され、矛盾が存在するかどうか判断される。矛盾が存在すると判断された場合、各種処理部9により、上記第1の実施の形態と同様な各種処理

が行なわれる。これにより、本実施の形態においても第1の実施の形態と同様な効果が得られる。

【0133】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0134】図2に示すネットワークを例にして、本実施の形態のネットワーク監視装置41の判断部8による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置41からなる。ID=6のノード206とID=7のノード207とID=9のノード209から連続したパケットが送出された場合、そのパケットの順番は、ID=6のノード206、ID=7のノード207、ID=9のノード209であるはずである。これ以外の順番の連続パケットが観測された場合、矛盾が存在することになる。

【0135】また、その矛盾した順番が、ID=7のノード207、ID=9のノード209、ID=6のノード206であった場合、ID=7のノード207とID=9のノード209の順番は正しいが、ID=6のノード206の順番が不自然であることが解る。

【0136】ここから、ID=6のノード206がなりすまされている可能性があることが解り、またトポロジ情報から、なりすましを行っているノードは、ID=9のノード206よりもルートよりのノード、図2の場合はID=10のノード210である可能性があることが解る。

【0137】以上のように、本発明の第7の実施の形態のネットワーク監視装置41は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、連続したパケットを受信した際に、受信したパケットのソースIDとその受信順番を識別するソース順番識別部13と、トポロジ記憶部6に記憶されたトポロジ情報と、ソース順番識別部13で識別されたパケットのソースIDとその受信順番とを比較し、矛盾が存在するかどうかを判断する判断部8と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

(第8の実施の形態)

【0138】図9は、本発明の第8の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第2の実施の形態とは、ステップS102およびS103の替わりに、ステップS131乃至ステップS133を設けた点が主に相違している。

【0139】同図に示すように、ステップS101にお

いて、ネットワークのトポロジ情報を獲得する。次いでステップS104において、バスリセットの発生を待機する。ステップS104において、バスリセットが検出された場合、ステップS101へ戻り、検出されない場合はステップS131へ進む。ステップS131において、連続パケットの受信を待機する。ステップS131において、パケットが受信されない場合は、ステップS104へ戻り、パケットが受信された場合、ステップS132へ進む。

【0140】ステップS132において、パケットを受信した順番とパケットのソースIDを識別する。次いでステップS133において、ステップS101で獲得したトポロジ情報とステップS132で識別したパケットのソースIDとパケットを受信した順番とを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップS105で各種処理を行う。ステップS105における各種処理は、図3に示された上記第2の実施の形態におけるステップS105の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第2の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップS104へ戻る。ステップS105の各種処理が終了した後も、ステップS104へ戻る。

【0141】図2に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップS133における判断の方法を説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置41からなる。ID=6のノード206とID=7のノード207とID=9のノード209から連続したパケットが送出された場合、そのパケットの順番は、ID=6のノード206、ID=7のノード207、ID=9のノード209であるはずである。これ以外の順番の連続パケットが観測された場合、矛盾が存在することになる。

【0142】また、その矛盾した順番が、ID=7のノード207、ID=9のノード209、ID=6のノード206であった場合、ID=7のノード207とID=9のノード209の順番は正しいが、ID=6のノード206の順番が不自然であることが解る。

【0143】ここから、ID=6のノード206がなりすまされている可能性があることが解り、またトポロジ情報から、なりすましを行っているノードは、ID=9のノード206よりもルートよりのノード、図2の場合はID=10のノード210である可能性があることが解る。

【0144】以上のように、本発明の第8の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、連続したパケットを受信した際に、受信したパケットのソースIDとその受信順番を識別し、記憶されたトポロジ情報と、識別されたパケットのソースID

Dとその受信順番との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

(第9の実施の形態)

【0145】図10は、本発明の第9の実施の形態のネットワーク監視装置51の概略ブロック図を示す。これは上記第1の実施の形態とは、応答時間記憶部7の替わりに、ACKソース識別部14を設けた点が相違している。第1の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0146】ACKソース識別部14は、ACKに連続したパケットを受信した際に、ACKとそれに連続したパケットのソースIDとその受信順番を識別するものである。

【0147】以下に、本実施の形態のネットワーク監視装置51の動作を説明する。

【0148】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、ACKソース順番識別部14により、ACKに連続したパケットが受信され、ACKとそれに連続したパケットのソースIDとその受信順番が識別される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、ACKソース順番識別部14に識別されたACKとパケットのソースIDとその受信順番とが比較され、矛盾が存在するかどうか判断される。矛盾が存在すると判断された場合、各種処理部9により、上記第1の実施の形態と同様な各種処理が行なわれる。これにより、本実施の形態においても第1の実施の形態と同様な効果が得られる。

【0149】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0150】図2に示すネットワークを例にして、本実施の形態のネットワーク監視装置51の判断部8による判断の方法を以下に説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置51からなる。

【0151】ID=7のノード207から送出されたACKにパケットを連続できるのは、トポロジ上、ID=9のノード209とID=10のノード210のみである。それ以外のソースIDを持つパケットが、ID=7のノード207のACKに連続していた場合、矛盾が存在することになる。ID=7のノード207のACKに、ソースIDがID=6のノード206であるパケットが連続していた場合、ID=6のノード206はなりすまされている可能性があることが解る。また、なりす

ましを行っているノードは、ID=9のノード209またはID=10のノード210である可能性があることが解る。

【0152】以上のように、本発明の第9の実施の形態のネットワーク監視装置51は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、ACKに連続したパケットを受信した際に、ACKとそれに連続したパケットのソースIDとその受信順番を識別するACKソース識別部14と、トポロジ記憶部6に記憶されたトポロジ情報と、ACKソース識別部14で識別されたパケットのソースIDとその受信順番とを比較し、矛盾が存在するかどうかを判断する判断部8と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補を発見することができる。

(第10の実施の形態)

【0153】図11は、本発明の第10の実施の形態のネットワーク監視方法を示すフローチャートを示す。これは上記第2の実施の形態とは、ステップS102およびS103の替わりに、ステップS141乃至ステップS143を設けた点が主に相違している。

【0154】同図に示すように、ステップS101において、ネットワークのトポロジ情報を獲得する。次いでステップS104において、バスリセットの発生を待機する。ステップS104において、バスリセットが検出された場合、ステップS101へ戻り、検出されない場合はステップS141へ進む。ステップS141において、ACKに連続したパケットの受信を待機する。ステップS141において、パケットが受信されない場合は、ステップS104へ戻り、パケットが受信された場合は、ステップS142へ進む。

【0155】ステップS142において、ACKとパケットのソースIDを識別する。次いでステップS143において、ステップS101で獲得したトポロジ情報とステップS142で識別したACKとパケットのソースIDとを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップS105に進み、各種処理を行う。ステップS105における各種処理は、図3に示された上記第2の実施の形態におけるステップS105の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第2の実施の形態と同様な効果が得られる。矛盾が存在しなかった場合は、ステップS104へ戻る。ステップS105の各種処理が終了した後も、ステップS104へ戻る。

【0156】図2に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップS143における判断の方法を説明する。同図に示すように、このネットワークは、ノード201～210とネットワーク監視装置51からなる。

【0157】ID=7のノード207から送出されたACKにパケットを連続できるのは、トポロジ上ID=9のノード209とID=10のノード210のみである。それ以外のソースIDを持つパケットが、ID=7のノード207のACKに連続していた場合、矛盾が存在することになる。ID=7のノード207のACKに、ソースIDがID=6のノード206であるパケットが連続していた場合、ID=6のノード206はなりすまされている可能性があることが解る。また、なりすましを行っているノードは、ID=9のノード209またはID=10のノード210である可能性があることが解る。

【0158】以上のように、本発明の第10の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、ACKに連続したパケットを受信した際に、受信したACKとそれに連続したパケットのソースIDとその受信順番を識別し、記憶されたトポロジ情報と、識別されたACKとパケットのソースIDとその受信順番との整合性を判断するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

(第11の実施の形態)

【0159】図12は、本発明の第11の実施の形態のネットワーク監視装置61の概略ブロック図を示す。これは図6に示す上記第5の実施の形態とは、さらにルーティングテーブル確認部15を設けた点が相違している。上記の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0160】ルーティングテーブル確認部15は、判断部8と送受信部5に接続され、判断部8で矛盾が存在しないと判断され、かつ判断部8を介して得られたソースIDが仮想ノードIDであった場合、ブリッジなどのネットワーク中継機器のルーティングテーブルを取得するものである。

【0161】以下に、本実施の形態のネットワーク監視装置61の動作を説明する。

【0162】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、応答時間記憶部7により、送受信部5を介してネットワーク上のノードにpingが実行され、ネットワーク監視装置61とその他のノードとの間のping時間が記憶される。ここで、pingを行う順番はどのようなものでも構わない。

【0163】次に、ソース識別部11により、パケットが受信され、パケットのソースIDとパケットを受信したポートが識別される。さらに、時間測定部12により、送受信部5を介してバス上の状態が変化した時間が測定される。判断部8により、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶された

ping時間情報と、ソース識別部11に識別されたソースID情報と、時間測定部12が測定したバス状態時間測定情報とが比較され、矛盾が存在するかどうか判断される。矛盾が存在すると判断された場合、各種処理部9により、上記第1の実施の形態と同様な各種処理が行なわれる。これにより、本実施の形態においても第1の実施の形態と同様な効果が得られる。

【0164】上記のトポロジ情報の収集およびpingの実施は、設定された時間毎に行なわれても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行なわれても良い。バスリセット発生毎に行なわれるのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0165】また、ソースIDが仮想ノードIDであった場合、そのパケットを送出したノードはブリッジ、ルータ等のネットワーク中継機器である。矛盾が存在しないと判断され、かつソースIDが仮想ノードIDであった場合、ルーティングテーブル確認部15は、ネットワーク中継機器のルーティングテーブルを取得する。その後、判断部8は、ソース識別部11のソースID情報と、ルーティングテーブル確認部15のルーティングテーブル情報とを比較し、矛盾が存在するかどうかを判断する。矛盾が存在すると判断された場合、各種処理部9が処理を行う。尚、ルーティングテーブルをキャッシュしておくことで、毎回ルーティングテーブルを獲得に行く必要をなくしても良い。

【0166】以上のように、本発明の第11の実施の形態のネットワーク監視装置61は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、pingを実行して、得られたping時間を記憶する応答時間記憶部7と、送受信部5を介してパケットを受信した際に、そのパケットのソースIDとパケットを受信したポートを識別するソース識別部11と、送受信部5を介してバス上の状態が変化した時間を測定する時間測定部12と、トポロジ記憶部6に記憶されたトポロジ情報と、応答時間記憶部7に記憶されたping時間情報と、ソース識別部11で識別されたソースIDと、時間測定部12で測定された時間とを比較し、矛盾が存在するかどうかを判断する判断部8と、判断部8で矛盾が存在しないと判断され、かつ判断部8を介して得られたソースIDが仮想ノードIDであった場合、ブリッジなどのネットワーク中継機器のルーティングテーブルを取得するルーティングテーブル確認部15と、各種処理部9とを備えているので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

(第12の実施の形態)

【0167】図13は、本発明の第12の実施の形態のネットワーク監視方法を示すフローチャートを示す。こ

れは図7に示す上記第6の実施の形態とは、さらにステップS151乃至ステップS153を設けた点が相違している。

【0168】同図に示すように、ステップS101において、ネットワークのトポロジ情報を獲得する。次いでステップS102において、ネットワーク上のノードについてpingを実行し、ping時間を獲得する。次いで、ステップS104において、バスリセットの発生を待機する。ステップS104において、バスリセットが検出されなかった場合、ステップS101へ戻り、検出された場合は、ステップS121へ進む。

【0169】ステップS121において、バス状態の変化時間を測定する。次いでステップS122において、パケットを受信したポートとパケットのソースIDを識別する。次いでステップS123において、ステップS101で獲得したトポロジ情報と、ステップS102で獲得した応答時間と、ステップS121で測定したバス状態の変化時間情報と、ステップS122で識別したパケットのソースID情報とが比較され、矛盾が存在するかどうかを判断する。矛盾が存在しなかった場合は、ステップS151へ進み、ソースノードがブリッジであるか否かを判定する。ブリッジでなかった場合は、ステップS104へ戻り、ブリッジであった場合、ステップS152でルーティングテーブルを獲得する。ルーティングテーブルとパケットのソースIDを比較し、矛盾が存在するかどうかを判断する。矛盾が存在した場合、ステップS105で各種処理を行う。ステップS105における各種処理は、図3に示された上記第2の実施の形態におけるステップS105の各種処理と同様であるので、詳細な説明は省略する。これにより、本実施の形態においても第2の実施の形態と同様な効果が得られる。一方、矛盾が存在しなかった場合は、ステップS104へ戻る。ステップS105の各種処理が終了した後も、ステップS104へ戻る。

【0170】ここで、ブリッジとはルーティングテーブルと、パケットの中継機能を備えた機器を指す。尚、ルーティングテーブルをキャッシュしておくことで、毎回ルーティングテーブルを獲得に行く必要をなくしても良い。

【0171】以上のように、本発明の第12の実施の形態のネットワーク監視方法は、ネットワークのトポロジ情報を記憶し、pingを実行して、得られたping時間を記憶し、パケットを受信したポートを識別し、受信したパケットのソースIDを識別し、バス上の状態が変化した時間を測定し、記憶されたトポロジ情報と、記憶されたping時間と、識別された記憶されたソースIDと、測定された時間との整合性を判断し、識別されたソースIDがローカルバス以外のバスを示していた場合に、ブリッジの持つルーティングテーブルを確認し、ソースIDとルーティングテーブルとが矛盾する場合を

発見するので、ネットワーク上のノードの中から、なりすまされているノードと、なりすましを行っているノードの候補とを発見することができる。

(第13の実施の形態)

【0172】図14は、本発明の第13の実施の形態のリピータ装置71の概略ブロック図を示す。同図に示すように、本実施の形態のリピータ装置71は、送受信部5と、トポロジ記憶部6と、デスティネーション識別部16と、ポート制御部17を備えている。第1の実施の形態と同じ構成には同じ符号を付し、詳細な説明は省略する。

【0173】デスティネーション識別部16は、送受信部5がパケットを受信した際に、パケットのデスティネーションIDを識別するものである。ポート制御部17は、トポロジ記憶部6に記憶されたトポロジ情報と、デスティネーション識別部16で識別されたデスティネーションID情報とから、ポートの状態を判断し、パケットのリピートに関するポートの制御を行うものである。

【0174】以下に、本実施の形態のリピータ装置71の動作を説明する。

【0175】始めに、ネットワークのトポロジ情報が送受信部5を介して収集され、トポロジ記憶部6に記憶される。次に、送受信部5によりパケットが受信されると、デスティネーション識別部16により、パケットのデスティネーションIDが識別される。次に、ポート制御部17により、トポロジ記憶部6に記憶されたネットワークのトポロジ情報と、デスティネーション識別部16に識別されたデスティネーションID情報とから、ポートの状態が判断され、パケットのリピートに関するポートが制御される。ポート制御の方法については後述する。

【0176】上記のトポロジ情報の収集は、設定された時間毎に行っても良いし、トラフィック量が閾値以下の場合等の条件を設定し、条件が満たされた場合に行っても良い。バスリセット発生毎に行うのが、情報不足を回避しつつ情報収集回数を少なくするという点で好ましい。

【0177】図2に示すネットワークを例にして、本実施の形態のリピータ装置71のポート制御部17におけるポート制御の方法を以下に説明する。同図に示すように、このネットワークは、ノード201～210とリピータ装置71からなる。

【0178】パケットのデスティネーションIDが3であった場合、このパケットはID=3のノード204が接続されているポートP2のみにリピートすれば、パケットの役割を果たすことができるため、それ以外のポート、ポートP0およびポートP1にはリピートする必要はない。

【0179】しかし、バスを占有していることを示すために、何らかのデータをドライブする必要がある。そこ

でポート制御部17は以下のようにポートを制御する。

【0180】ポートP2は通常どおりにパケットのリピートを行う。パケットを受信したポートには通常どおりにリピートを行わない。ポートP0およびポートP1には、パケットと同サイズのダミーをリピートする。ダミーとしては、パケットのデータペイロード等重要と思われる部分を書き換えたもの、あるいは、あらかじめ用意してある無害なパケットが考えられ、またパケットでなくdata prefixを出しつづけても良い。

【0181】以上のように、本発明の第13の実施の形態のリピータ装置は、送受信部5と、この送受信部5を介して収集されたネットワークのトポロジ情報を記憶するトポロジ記憶部6と、送受信部5がパケットを受信した際に、パケットのデスティネーションIDを識別するデスティネーション識別部16と、トポロジ記憶部6に記憶されたトポロジ情報と、デスティネーション識別部16で識別されたデスティネーションID情報とから、ポートの状態を判断し、パケットのリピートに関するポートを制御するポート制御部17とを備えているので、パケット内容を、ソースノードとデスティネーションノード間経路上のノード以外のノードに流さないようにすることが可能になり、パケット内容を盗聴される可能性を減ずることができる。

(第14の実施の形態)

【0182】図15は、本発明の第14の実施の形態のリピート方法を示すフローチャートを示す。同図に示すように、ステップS101において、ネットワークのトポロジ情報を獲得する。ステップS104において、バスリセットの発生を待機する。ステップS104において、バスリセットが検出された場合、ステップS101へ戻り、検出されない場合はステップS161へ進む。ステップS161において、パケットの受信を待機する。ステップS161において、パケットが受信されない場合は、ステップS104へ戻り、パケットが受信された場合、ステップS162へ進む。ステップS162において、ポートのリピートを後述するように制御する。

【0183】図2に示すネットワークを例にして、本実施の形態のネットワーク監視方法のステップS162におけるポート制御の方法を説明する。同図に示すように、このネットワークは、ノード201～210とリピータ装置71からなる。

【0184】パケットのデスティネーションIDが3であった場合、このパケットはID=3のノード204が接続されているポートP2のみにリピートすれば、パケットの役割を果たすことができるため、それ以外のポート、ポートP0およびポートP1にはリピートする必要はない。

【0185】しかし、バスを占有していることを示すために、何らかのデータをドライブする必要はある。そこ

でポート制御部17は以下のようにポートを制御する。

【0186】ポートP2は通常どおりにパケットのリピートを行う。パケットを受信したポートには通常どおりにリピートを行わない。ポートP0およびポートP1には、パケットと同サイズのダミーをリピートする。ダミーとしては、パケットのデータペイロード等重要と思われる部分を書き換えたもの、あらかじめ用意してある無害なパケット、が考えられ、またパケットでなくdata prefixを出しつづけても良い。

【0187】以上のように、本発明の第14の実施の形態のリピート方法は、ネットワークのトポロジ情報を記憶し、パケットのデスティネーションIDを識別し、記憶されたトポロジ情報と、識別されたデスティネーションID情報とから、ポートの状態を判断し、パケットのリピートに関するポートを制御するので、パケット内容をソースノードとデスティネーションノード間経路上のノード以外のノードに流さないようにすることが可能になり、パケット内容を盗聴される可能性を減ずることができる。

(第15の実施の形態)

【0188】本発明の第15の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、警告発生時状態を収集する情報収集部(図示無し)と、この収集された情報をユーザに通知する表示部(図示無し)とを備えている。

【0189】ここで表示する内容は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのID、名前、トポロジ上の位置、システム上の位置、警告を出したノードのID、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容および、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在をユーザに示すことができる。

(第16の実施の形態)

【0190】本発明の第16の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、警告内容と警告発生時の状態をユーザに通知するよう表示する。

【0191】ここで表示する内容は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのID、名前、トポロジ上の位置、システム上の位置、警告を出したノードのID、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容および、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在をユーザに示すことができる。

(第17の実施の形態)

【0192】本発明の第17の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部（図示無し）と、警告発生時状態を収集する情報収集部（図示無し）と、公衆回線に接続された公衆回線通信部（図示無し）とを備えている。

【0193】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、警告内容を公衆回線に伝送する。

【0194】電話回線を利用して電話、携帯電話、PHS、ページャ等に接続して異常を知らせても良い。また、必要な情報を音声メッセージに変換して、電話、携帯電話、PHS等で情報を知らせても良い。さらに、コードに変換して携帯電話、PHS、ページャ等に表示させる、画像にしてFAX信号にて伝送しても良い。

【0195】また、インターネットを利用して、電子メール、常時接続型のアプリケーション、プッシュ配信型のアプリケーション、Webサーバ等を用いて必要な情報を伝達しても良い。これにより、不正な機器の存在を遠隔地のユーザに示すことができる。

（第18の実施の形態）

【0196】本発明の第18の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、警告内容を公衆回線に伝送する。

【0197】電話回線を利用して電話、携帯電話、PHS、ページャ等に接続して異常を知らせても良い。また、必要な情報を音声メッセージに変換して、電話、携帯電話、PHS等で情報を知らせても良い。さらに、コードに変換して携帯電話、PHS、ページャ等に表示させる、画像にしてFAX信号にて伝送しても良い。

【0198】また、インターネットを利用して、電子メール、常時接続型のアプリケーション、プッシュ配信型のアプリケーション、Webサーバ等を用いて必要な情報を伝達しても良い。これにより、不正な機器の存在を遠隔地のユーザに示すことができる。

（第19の実施の形態）

【0199】本発明の第19の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部（図示無し）と、警告発生時状態を収集する情報収集部（図示無し）と、情報を記録する記憶部（図示無し）とを備えている。

【0200】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、警告の内容と警告発生時の状態等の情

報を記録する。

【0201】ここで記録する情報は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのID、名前、トポロジ上の位置、システム上の位置、警告を出したノードのID、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在を記録し、後から参照できる。

（第20の実施の形態）

【0202】本発明の第20の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、情報を記録する。

【0203】ここで記録する情報は、警告の根拠、時刻、ネットワークトポロジ、システム図、不正なノードのID、名前、トポロジ上の位置、システム上の位置、警告を出したノードのID、名前、トポロジ上の位置、システム上の位置、警告のあったパケットの内容、現在流れているパケットの内容、警告以外に行った処理の内容等が考えられる。これにより、不正な機器の存在を記録し、後から参照できる。

（第21の実施の形態）

【0204】本発明の第21の実施の形態のネットワーク装置（図示無し）は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部（図示無し）と、警告に関連する機器の挙動または状態を収集する情報収集部（図示無し）と、情報を記録する記憶部（図示無し）とを備えている。

【0205】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録する。記録は、不正な機器をブラックリストとして登録し、さらにブラックリスト上の機器を監視する。

【0206】ここで監視内容としては、機器に関連するパケットを監視および記録しても良いし、機器のレジスタを一定間隔、またはバスリセット毎に取得および記録しても良い。また、ブラックリストの管理は、一定時間不正が発見されなかった場合リストから消去しても良いし、機器認証を行い正常であることが確認された後リストから消去しても良い。あるいは、ネットワークから削除されたのを確認したらリストから消去しても良い。リストから消去する代わりに、休眠状態にする、監視のレベルを変化させても良い。これにより、不正な機器の存在およびその挙動を記録し、後から参照でき、不正な挙動を発見できる。

（第22の実施の形態）

【0207】本発明の第22の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、警告に関連した何れかまたは全ての機器の挙動を記録する、または機器の状態を記録する。記録は、不正な機器をブラックリストとして登録し、さらにブラックリスト上の機器を監視する。

【0208】ここで監視内容としては、機器に関連するパケットを監視および記録しても良いし、機器のレジスタを一定間隔、またはバスリセット毎に取得および記録しても良い。また、ブラックリストの管理は、一定時間不正が発見されなかった場合リストから消去しても良いし、機器認証を行い正常であることが確認された後リストから消去しても良い。あるいは、ネットワークから削除されたのを確認したらリストから消去しても良い。リストから消去する代わりに、休眠状態にする、監視のレベルを変化させても良い。これにより、不正な機器の存在およびその挙動を記録し、後から参照でき、不正な挙動を発見できる。

(第23の実施の形態)

【0209】本発明の第23の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、他機器にサービスを提供するサービス処理部と、条件によりサービスの提供の許可を行うサービス制御部とを備えている。

【0210】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、サービスを停止する。ここでサービスの停止とは、警告に関連した機器の何れかまたは全てのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することである。

【0211】サービス停止としては、不正な機器との間に張られているコネクションを切断しても良いし、不正な機器からのアクセスを許可しないようにしても良いし、不正な機器からのパケットを受信しないようにしても良い。あるいは、サービス停止の代わりにサービスを変更しても良い。サービス変更とは、アクセスレベルを制限する、サービス内容を制限する、または不正な機器専用のサービスを用意しておき供給する等が考えられる。これにより、不正な機器に供与するサービスに制限を与え、不正な機器による被害を制限できる。

(第24の実施の形態)

【0212】本発明の第24の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、サービスを停止する。

【0213】ここでサービスの停止とは、警告に関連した機器の何れかまたは全てのアクセス、サービス要求を設定した条件が満たされるまで拒否する、または設定されたものに変更することである。

【0214】サービス停止としては、不正な機器との間に張られているコネクションを切断しても良いし、不正な機器からのアクセスを許可しないようにしても良いし、不正な機器からのパケットを受信しないようにしても良い。あるいは、サービス停止の代わりにサービスを変更しても良い。サービス変更とは、アクセスレベルを制限する、サービス内容を制限する、または不正な機器専用のサービスを用意しておき供給する等が考えられる。これにより、不正な機器に供与するサービスに制限を与え、不正な機器による被害を制限できる。

(第25の実施の形態)

【0215】本発明の第25の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、パケットのルーティングを行うルーティング部(図示無し)と、ルーティングの設定を行うルーティング制御部(図示無し)とを備えている。

【0216】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、警告に関連した機器の何れかまたは全てのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更する。

【0217】例として、不正な機器に関連するルーティングを停止する。あるいは停止する代わりに、通常は不正な機器にルーティングされるべきパケットを、不正機器を監視している機器にルーティングするようにしても良い。また、不正な機器から送出されたパケットを、同様に不正機器を監視している機器にルーティングするようにしても良い。あるいは上記パケットを通常のルーティング経路とは異なる、不正ノード用の経路にルーティングをするようにしても良いし、特定のエリアには不正ノード関連のパケットを侵入させないようにしても良い。

【0218】これにより、不正な機器からのパケットのルーティングをコントロールでき、記録が容易に行える、あるいは不正な機器による被害を制限できる。

(第26の実施の形態)

【0219】本発明の第26の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、警告に関連した機器の何れかまたは全てのパケットのルーティングを設定した条件が満たされるまで停止する、または設定された条件に変更する。



【0220】例として、不正な機器に関連するルーティングを停止する。あるいは停止する代わりに、通常は不正な機器にルーティングされるべきパケットを、不正機器を監視している機器にルーティングするようにしても良い。また、不正な機器から送出されたパケットを、同様に不正機器を監視している機器にルーティングするようにしても良い。あるいは上記パケットを通常のルーティング経路とは異なる、不正ノード用の経路にルーティングをするようにしても良いし、特定のエリアには不正ノード関連のパケットを侵入させないようにしても良い。

【0221】これにより、不正な機器からのパケットのルーティングをコントロールでき、記録が容易に行える、あるいは不正な機器による被害を制限できる。

(第27の実施の形態)

【0222】本発明の第27の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、機器の認証機能を備えた機器認証部とを備えている。

【0223】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、関連する機器に対し機器認証を行う、またはやり直す。

【0224】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0225】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

(第28の実施の形態)

【0226】本発明の第28の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、機器認証を行う、または機器認証をやり直す。

【0227】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0228】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

(第29の実施の形態)

【0229】本発明の第29の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、データの暗号化を行う暗号部とを備えている。

【0230】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、データの暗号化を行う、または暗号化キーを再作成する。

【0231】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

(第30の実施の形態)

【0232】本発明の第30の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、通信を暗号化する、または暗号化キーを作成し直すようにする。

【0233】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

【0234】

【発明の効果】以上説明したように、本発明はネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視方法を提供することができるものである。

【0235】また、本発明はネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視装置を提供することができるものである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図2】実施の形態の挙動を説明するためのネットワーク構成例を示すブロック図

【図3】本発明の第2の実施の形態のネットワーク監視方法を示すフローチャート

【図4】本発明の第3の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図5】本発明の第4の実施の形態のネットワーク監視方法を示すフローチャート

【図6】本発明の第5の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図7】本発明の第6の実施の形態のネットワーク監視方法を示すフローチャート

【図8】本発明の第7の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【0220】例として、不正な機器に関連するルーティングを停止する。あるいは停止する代わりに、通常は不正な機器にルーティングされるべきパケットを、不正機器を監視している機器にルーティングするようにしても良い。また、不正な機器から送出されたパケットを、同様に不正機器を監視している機器にルーティングするようにしても良い。あるいは上記パケットを通常のルーティング経路とは異なる、不正ノード用の経路にルーティングをするようにしても良いし、特定のエリアには不正ノード関連のパケットを侵入させないようにしても良い。

【0221】これにより、不正な機器からのパケットのルーティングをコントロールでき、記録が容易に行える、あるいは不正な機器による被害を制限できる。

(第27の実施の形態)

【0222】本発明の第27の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、機器の認証機能を備えた機器認証部とを備えている。

【0223】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、関連する機器に対し機器認証を行う、またはやり直す。

【0224】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0225】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

(第28の実施の形態)

【0226】本発明の第28の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、機器認証を行う、または機器認証をやり直す。

【0227】機器認証は、不正な機器の正当性を確認するために不正な機器に対して行なわれても良いし、あるいは不正な機器による影響を確認するために、不正な機器以外に行なわれても良い。

【0228】これにより、不正な機器の状態を把握できる、あるいは不正な機器の影響を把握できる。

(第29の実施の形態)

【0229】本発明の第29の実施の形態のネットワーク装置(図示無し)は、上記の実施の形態のネットワーク監視装置1、21、31、41、51および61の各種処理部9から警告を受ける警告受信部(図示無し)と、データの暗号化を行う暗号部とを備えている。

【0230】本実施の形態のネットワーク装置は、警告受信部を介してネットワーク監視装置1、21、31、41、51および61の各種処理部9の何れかから警告を受けた場合に、データの暗号化を行う、または暗号化キーを再作成する。

【0231】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

(第30の実施の形態)

【0232】本発明の第30の実施の形態のネットワーク保護方法は、上記の実施の形態のネットワーク監視方法のステップS105の各種処理で発生された警告を受けた場合に、通信を暗号化する、または暗号化キーを作成し直すようにする。

【0233】これにより、不正な機器にパケットを盗聴されることを防止し、またなりすましを防止することができる。

【0234】

【発明の効果】以上説明したように、本発明はネットワークのトポロジ情報を記憶し、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視方法を提供することができるものである。

【0235】また、本発明はネットワークのトポロジ情報を記憶するトポロジ記憶部と、この記憶されたトポロジ情報と矛盾するバス状態、バス状態の変化またはパケットを検出する検出部とを具備することにより、バス上に存在する機器が他の機器になりすまそうとしている可能性を発見することができるという優れた効果を有するネットワーク監視装置を提供することができるものである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図2】実施の形態の挙動を説明するためのネットワーク構成例を示すブロック図

【図3】本発明の第2の実施の形態のネットワーク監視方法を示すフローチャート

【図4】本発明の第3の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図5】本発明の第4の実施の形態のネットワーク監視方法を示すフローチャート

【図6】本発明の第5の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図7】本発明の第6の実施の形態のネットワーク監視方法を示すフローチャート

【図8】本発明の第7の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図9】本発明の第8の実施の形態のネットワーク監視方法を示すフローチャート

【図10】本発明の第9の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図１１】本発明の第１０の実施の形態のネットワーク監視方法を示すフローチャート

【図１２】本発明の第１１の実施の形態のネットワーク監視装置の構成を示す概略ブロック図

【図１３】本発明の第１２の実施の形態のネットワーク監視方法を示すフローチャート

【図 14】本発明の第 13 の実施の形態のリピータ装置の構成を示す概略ブロック図

【図15】本発明の第14の実施の形態のリPEAT方法を示すフローチャート

【符号の説明】

1、21、31、41、51、61 ネットワーク監視

## 装置

## 5 送受信部

## 6 トポロジ記憶部

## 7 応答時間記憶部

## 8 判断部

## 9 各種処理部

10 バス

P0、P1、P2 ポート

## 11 ソース識別部

12 時間測定部

### 13 ソース順番識別部

## 14 ACKソース順番識別部

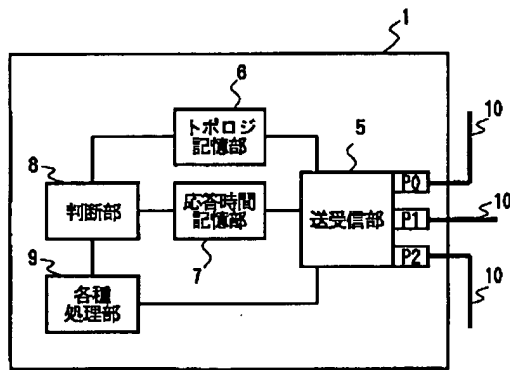
## 15 ルーティングテーブル確認部

## 16 デスティネーション識別部

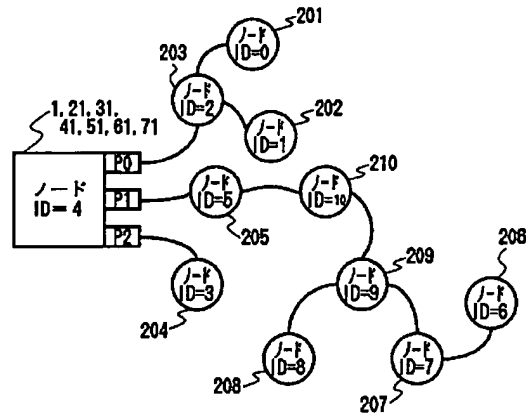
## 17 ポート制御部

## 71 リピータ装置

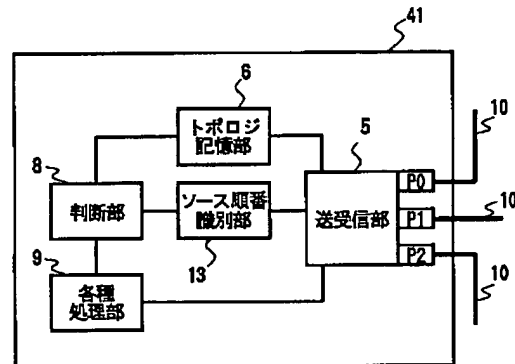
【図1】



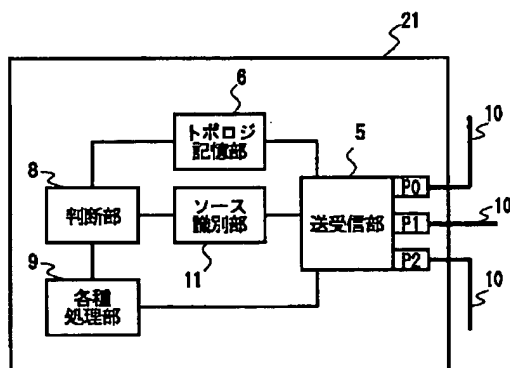
【図2】



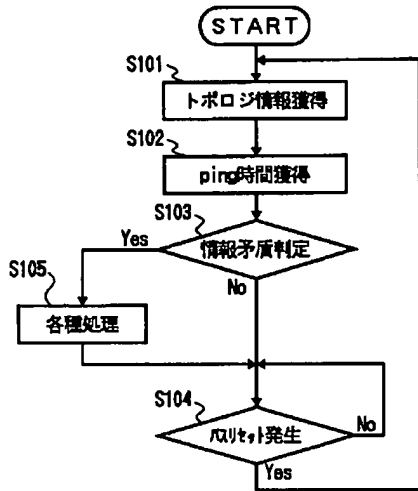
【図8】



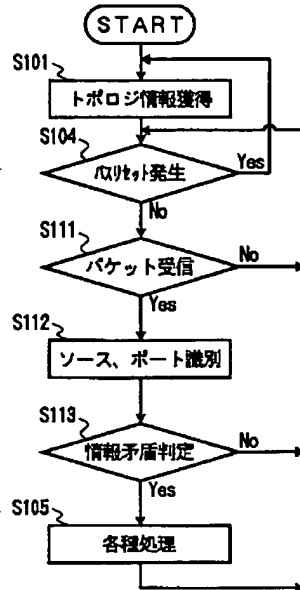
【図4】



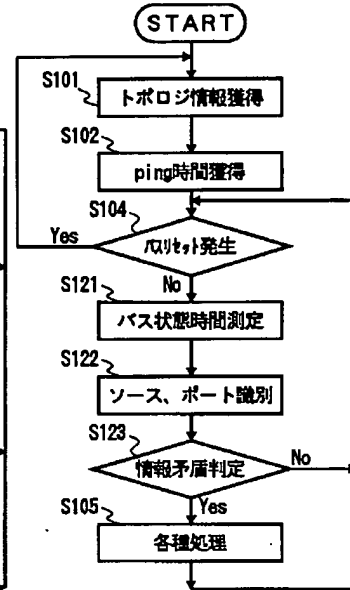
【図3】



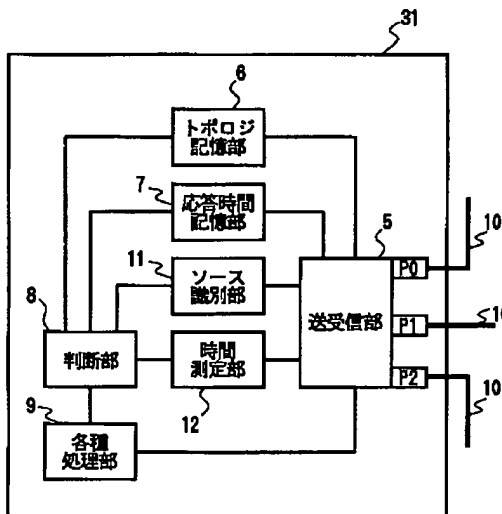
【図5】



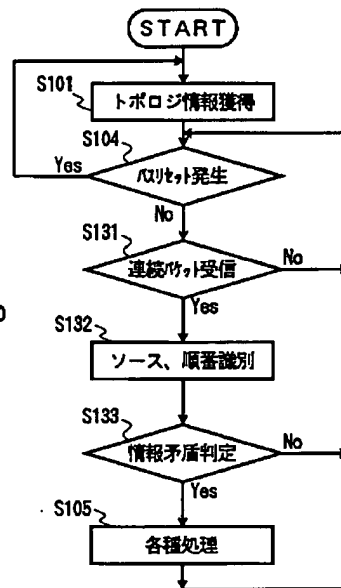
【図7】



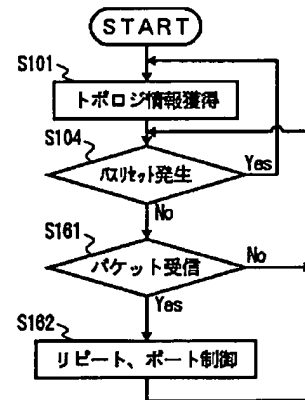
【図6】



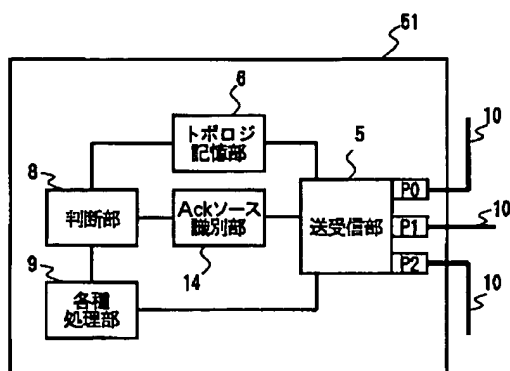
【図9】



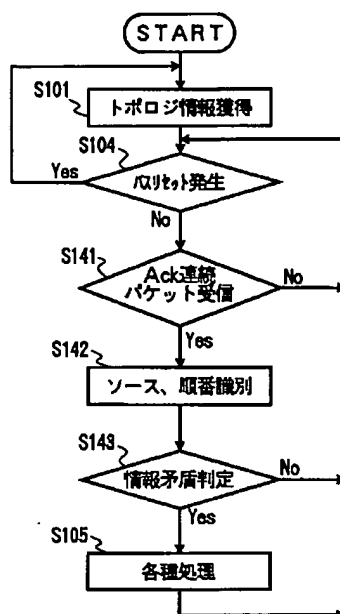
【図15】



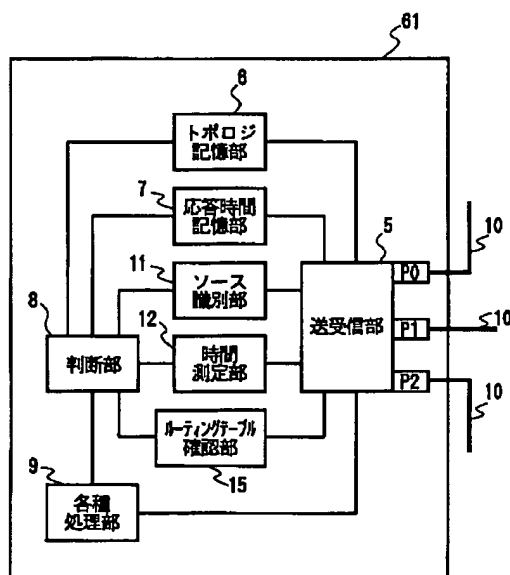
【図10】



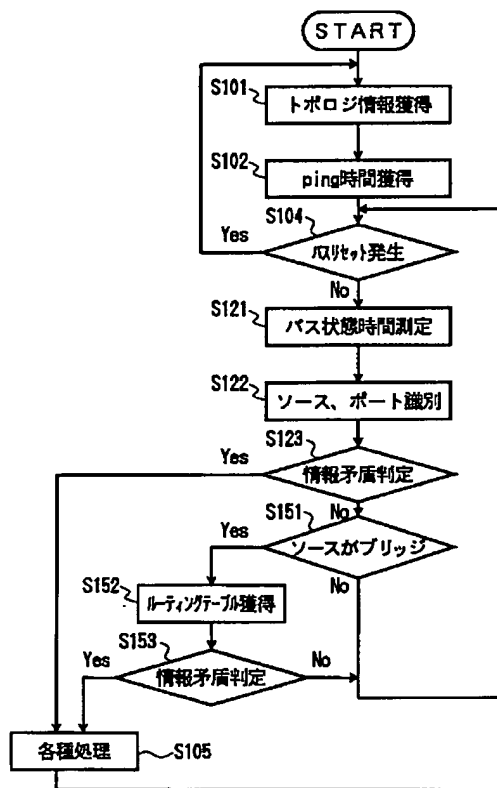
【図11】



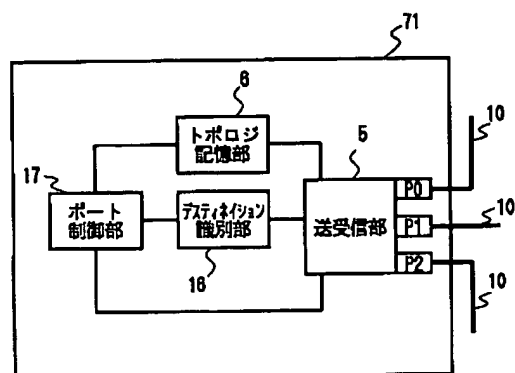
【図12】



【図13】



【図14】



フロントページの続き

Fターム(参考) 5K030 GA15 HA08 HB06 HB28 HB29  
KA07 LA02 MA06 MC04 MC06  
MC09  
5K033 AA08 CB04 CC01 DA13 DB20  
EA05  
5K035 EE03 EE05 GG01 MM02 MM06